WHAT IS CLAIMED IS:

1. A polynomial inverse computing apparatus comprising:

a plurality of registers including a first register, a second register, a third register, a fourth register, a fifth register, and a sixth register;

a left shift unit;

a first exclusive-OR unit and a second exclusive-OR unit;

a doubling computing unit configured to execute doubling computation in an extension field with characteristic 2;

a halving computing unit configured to execute halving computation in the extension field of characteristic 2;

a determination unit configured to determine whether or not a content of each of the registers is a zero value;

a decrement unit configured to decrement the content of each of the registers; and

an increment unit configured to increment the content of each of the registers.

2. The polynomial inverse computing apparatus according to claim 1, further comprising a controller which controls the left shit unit, the doubling computing unit, the first decrement unit, the second decrement unit, the increment unit, the first register,

the second register, the third register, the fourth register, the first exclusive-OR unit, the second exclusive-OR unit, the determination unit, and the halving computing unit in a first state that a most significant bit of the first register fails to be 1, a second state that the most significant bit of the first register is 1, and a third state after the second state finishes,

in the first state, a first series of operations are repeatedly performed,

the first series of operations including left-shift of a content of the first register by the left shift unit, doubling of a content of the third register by the doubling computing unit, decrement of a content of the fifth register by 1 by the first decrement unit, and increment of a content of the sixth register by 1 by the increment unit,

in the second state shifted from the first state if the most significant bit of the first register is 1, the first register and the second register store an output of the first exclusive-OR unit and the content of the first register, respectively, and the third register and the fourth register store an output of the second exclusive-OR unit and the content of the third register, respectively,

in the third state shifted from the second state after the second state finishes, unless the

determination unit determines that the content of the sixth register is a zero value, and as long as the most significant bit of the first register is 1, a second series of operations are repeatedly performed,

the second series of operations including storage of the output of the first exclusive-OR unit into the first register, storage of the output of the second exclusive-OR unit into the third register, decrement of the content of the sixth register by 1 by the second decrement unit, left-shift of the content of the first register by the left-shift unit, and halving of a content of the fourth register by the halving computing unit,

the third state being shifted to the first state if the determination unit determines that the content of the sixth register is the zero value and if the determination unit determines that the content of the fifth register is a non-zero value ,

the content of the fourth register being output as a result if the second determination unit determines that the content of the sixth register is the zero value and if the first determination unit determines that the content of the fifth register is the zero value.

3. The polynomial inverse computing apparatus according to claim 1, wherein:

if the most significant bit of the first register

is 1,

(a) the second register holds a content of the first register,

(b) the fourth register holds a content of the third register,

(c) the first exclusive-OR unit obtains a first exclusive-OR result of contents of the first register and the second register and outputs the first exclusive-OR result to the first register, and

(d) the second exclusive-OR unit obtains a second exclusive-OR result of contents of the third register and fourth register and outputs the second exclusive-OR result to the third register;

if the most significant bit of the first register is the zero value,

the left shift unit left-shifts the content of the first register,

the doubling computing unit executes doubling computation on the content of the third register in an extension field with characteristic 2,

the first decrement unit decrements a content of the fifth register, and

the second decrement unit decrements a content of the sixth register;

if the above-mentioned operations (a), (b), (c) and (d) are executed and if the content of the sixth register is a non-zero value and if a most significant

bit of the first register is 1, and then if the above-mentioned operations (c) and (d) are executed, the halving computing unit executes halving computation on a content of the fourth register in the extension field with characteristic 2, and the increment unit increments the content of the sixth register,

if the above-mentioned operations (a), (b), (c) and (d) are executed and if the content of the sixth register is the zero value, the first determination unit determines whether or not the content of the fifth register is the zero value; and

if the above-mentioned operations (a), (b), (c) and (d) are executed, the second determination unit determines whether or not the content of the sixth register is the zero value.

4. A polynomial inverse computing apparatus comprising:

a first register which stores a divisor as an initial value;

a second register which stores a modulo as an initial value and holds a content of the first register in a first condition;

a third register which stores a dividend as an initial value;

a fourth register which stores a zero value as an initial value and holds a content of the third register in the first condition;

a fifth register which stores a number of bits of the modulo as an initial value;

a sixth register which stores the zero value as an initial value;

a first exclusive-OR unit configured to obtain a first exclusive-OR result of contents of the first register and the second register and outputs the first exclusive-OR result to the first register in the first condition;

a second exclusive-OR unit configured to obtain a second exclusive-OR result of contents of the third register and the fourth register and outputs the second exclusive-OR result to the third register in the first condition;

a left shift unit configured to left-shift the content of the first register in a second condition;

a doubling computing unit configured to execute doubling computation on the content of the third register in an extension field with characteristic 2 in the second condition;

a first decrement unit configured to decrement a content of the fifth register in the second condition;

a second decrement unit configured to decrement a content of the sixth register in the second condition;

a halving computing unit configured to executes halving computation on a content of the fourth register in the extension field with characteristic 2 in a third

condition;

an increment unit configured to increment the content of the sixth register in the third condition;

a first determination unit configured to determine, in a fourth condition, whether or not the content of the fifth register is the zero value; and

a second determination unit configured to determine, in a fifth condition, whether or not the content of the sixth register is the zero value.

5. The polynomial inverse computing apparatus according to claim 4, wherein:

if a most significant bit of the first register is 1,

the second register holds the content of the first register,

the fourth register holds the content of the third register,

the first exclusive-OR unit obtains the first exclusive-OR result and outputs the first exclusive-OR result to the first register, and

the second exclusive-OR unit obtains the second exclusive-OR result and outputs the second exclusive-OR result to the third register.

6. The polynomial inverse computing apparatus according to claim 4, wherein:

if the most significant bit of the first register is the zero value,

the left shift unit left-shifts the content of the first register,

the doubling computing unit executes doubling computation on the content of the third register in an extension field with characteristic 2,

the first decrement unit decrements the content of the fifth register, and

the second decrement unit decrements the content of the sixth register.

7. The polynomial inverse computing apparatus according to claim 4, wherein:

if the following operations (a), (b), (c) and (d) are executed and if the content of the sixth register is a non-zero value and if a most significant bit of the first register is 1, and then if the following operations (c) and (d) are executed,

(a) the second register holds a content of the first register,

(b) the fourth register holds a content of the third register,

(c) the first exclusive-OR unit obtains a first exclusive-OR result of contents of the first register and the second register and outputs the first exclusive-OR result to the first register, and

(d) the second exclusive-OR unit obtains a second exclusive-OR result of contents of the third register and fourth register and outputs the second

exclusive-OR result to the third register,

the halving computing unit executes halving computation on a content of the fourth register in the extension field with characteristic 2, and the increment unit increments the content of the sixth register.

8. The polynomial inverse computing apparatus according to claim 4, wherein:

if the following operations (a), (b), (c) and (d) are executed and if the content of the sixth register is a non-zero value,

(a) the second register holds a content of the first register,

(b) the fourth register holds a content of the third register,

(c) the first exclusive-OR unit obtains a first exclusive-OR result of contents of the first register and the second register and outputs the first exclusive-OR result to the first register, and

(d) the second exclusive-OR unit obtains a second exclusive-OR result of contents of the third register and fourth register and outputs the second exclusive-OR result to the third register,

the first determination unit determines whether or not the content of the fifth register is the zero value.

9. The polynomial inverse computing apparatus

according to claim 4, wherein:

if the following operations (a), (b), (c) and (d) are executed and if the content of the sixth register is a non-zero value,

(a) the second register holds a content of the first register,

(b) the fourth register holds a content of the third register,

(c) the first exclusive-OR unit obtains a first exclusive-OR result of contents of the first register and the second register and outputs the first exclusive-OR result to the first register, and

(d) the second exclusive-OR unit obtains a second exclusive-OR result of contents of the third register and fourth register and outputs the second exclusive-OR result to the third register,

the second determination unit determines whether or not the content of the sixth register is the zero value.

the second determination unit determines whether or not the content of the sixth register is the zero value.

10. The polynomial inverse computing apparatus according to claim 4, wherein:

in a first state, unless a most significant bit of the first register is 1, a first series of operations are repeatedly performed,

the first series of operations including left-shift of the content of the first register by the left shift unit, doubling of the content of the third register by the doubling computing unit, decrement of the content of the fifth register by 1 by the first decrement unit, and increment of the content of the sixth register by 1 by the increment unit,

in a second state shifted from the first state if the most significant bit of the first register is 1, the first register and the second register store an output of the first exclusive-OR unit and the content of the first register, respectively, and the third register and the fourth register store an output of the second exclusive-OR unit and the content of the third register, respectively,

in a third state shifted from the second state after the second state finishes, unless the second determination unit determines that the content of the sixth register is the zero value, and as long as the most significant bit of the first register is 1, a second series of operations are repeatedly performed,

the second series of operations including storage of the output of the first exclusive-OR unit into the first register, storage of the output of the second exclusive-OR unit into the third register, decrement of the content of the sixth register by 1 by the second decrement unit, left-shift

of the content of the first register by the left-shift unit, and halving of the content of the fourth register by the halving computing unit,

the third state being shifted to the first state if the second determination unit determines that the content of the sixth register is the zero value and if the first determination unit determines that the content of the fifth register is a non-zero value,

the content of the fourth register being output as a result if the second determination unit determines that the content of the sixth register is the zero value and if the first determination unit determines that the content of the fifth register is the zero value.

11. The polynomial inverse computing apparatus according to claim 4, wherein if a most significant bit of the third register is 1, the doubling computing unit left-shifts the content of the third register by one bit and obtains an exclusive-OR result of the content of the third register and the modulo, and

if the most significant bit of the third register is the zero value, the doubling computing unit left-shifts the content of the third register by one bit.

12. The polynomial inverse computing apparatus according to claim 4, wherein if a least significant bit of the fourth register is 1, the halving computing

unit obtains an exclusive-OR result of the content of the fourth register and the modulo, and right-shifts the content of the fourth register by one bit, and

if the least significant bit of the fourth register is zero value, the halving computing unit right-shifts the content of the fourth register by one bit.

13. The polynomial inverse computing apparatus according to claim 4, wherein the fifth register is formed of a one-hot counter.

14. The polynomial inverse computing apparatus according to claim 4, wherein the sixth register is formed of a one-hot counter.

15. A multiplier apparatus comprising:

a plurality of registers including a first register, a second register, a third register, and a fourth register,

the first register, the second register, the third register, and the fourth register store a multiplier, a zero value, a multiplicand, and a modulo, respectively, the registers being used for a polynomial inverse computing apparatus;

a determination unit configured to determine whether or not a content of the fourth register is the zero value;

if the determination unit determines the content of the fourth register is a non-zero value,

a decrement unit configured to decrement the content of the fourth register;

a doubling computing unit configured to execute doubling computation in an extension field with characteristic 2 to the second register;

a left shift unit configured to left-shift the content of the first register;

if a most significant bit of the first register is 1,

a exclusive-OR unit configured to obtain a exclusive-OR result of contents of the second register and the third register and output the exclusive-OR result to the second register; and

an output unit configured to output a content of the second register if the determination unit determines the content of the fourth register is the zero value.

16. The multiplier apparatus according to claim 15, wherein: if the first register, the second register, the third register, and the fourth register are used for a polynomial inverse computing apparatus,

the first register stores a divisor as an initial value,

the second register stores a dividend as an initial value,

the third register stores zero value as an initial value and holds a content of the second register, and

the fourth register stores a number of bits of the modulo as an initial value.

17. A polynomial inverse computing method comprising:

storing, as initial values into a first register, a second register, a third register, a fourth register, a fifth register, and a sixth register, a divisor, a modulo, a dividend, a zero value, a number of bits of the modulo and the zero value, respectively;

in a first state, unless a most significant bit of the first register is 1, repeatedly performing a first series of operations, the first series of operations including

left-shifting a content of the first register,

doubling a content of the third register,

decrementing a content of the fifth register by 1, and

incrementing a content of the sixth register by 1,

the first state being;

in a second state shifted from the first state if the most significant bit of the first register is 1,

storing an output of a first exclusive-OR unit which inputs contents of the first register and the second register, and the content of the first

register into the first register and the second register, respectively, and

storing a second exclusive-OR unit which inputs contents of the third register and the fourth register, and the content of the third register into the third register and the fourth register, respectively,

in a third state shifted from the second state after the second state finishes, unless the content of the sixth register is the zero value, and as long as the most significant bit of the first register is 1, repeatedly performing a second series of operations, the second series of operations including

storing the output of the first exclusive-OR unit into the first register,

storing the output of the second exclusive-OR unit into the third register,

decrementing the content of the sixth register by 1, left-shifting the content of the first register, and

halving the content of the fourth register,

the third state being shifted to the first state if the content of the sixth register is the zero value and if the content of the fifth register is non-zero value,

the content of the fourth register being output as

a result if the content of the sixth register is the zero value and if the content of the fifth register is the zero value.

18. The polynomial inverse computing method according to claim 17, wherein in the doubling, if the most significant bit is 1, the content of the third register is left-shifted by one bit, and an exclusive-OR result of the content of the third register and the modulo is obtained, and

if the most significant bit of the third register is the zero value, the content of the third register is left-shifted by one bit.

19. The polynomial inverse computing method according to claim 17, wherein in the halving, if a least significant bit of the fourth register is 1, an exclusive-OR result of the content of the fourth register and the modulo is obtained, and the content of the fourth register is right-shifted by one bit, and

if the least significant bit of the fourth register is the zero value, the content of the fourth register is right-shifted by one bit.